Docket No.: P2001,0019

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : BERNDT GAMMEL ET AL.

Filed : CONCURRENTLY HEREWITH

Title : CACHE MEMORY AND METHOD FOR ADDRESSING

CLAIM FOR PRIORITY

Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450

Sir:

Claim is hereby made for a right of priority under Title 35, U.S. Code, Section 119, based upon the German Patent Application 101 01 552.6, filed January 15, 2001.

A certified copy of the above-mentioned foreign patent application is being submitted herewith.

Respectfully submitted,

LAURENCE A. GREENBERG REG. NO. 29.308

Date: July 15, 2003

Lerner and Greenberg, P.A. Post Office Box 2480 Hollywood, FL 33022-2480

Tel: (954) 925-1100 Fax: (954) 925-1101

/kf

BUNDESREPUBLIK DEUTSCHLAND



Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:

101 01 552.6

Anmeldetag:

15. Januar 2001

Anmelder/Inhaber:

Infineon Technologies AG, München/DE

Bezeichnung:

Cache-Speicher und Verfahren zur Adressierung

IPC:

G 06 F 12/08

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 26. Juni 2003

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

your

Jerofsky

Beschreibung

Cache-Speicher und Verfahren zur Adressierung

5 Die vorliegende Erfindung betrifft einen Cache-Speicher, der auf einem Security-Controller verwendet wird.

Cache-Speicher sind im allgemeinen relativ kleine, aber schnelle Pufferspeicher, die eingesetzt werden, um die La-10 tenzzeit beim Zugriff eines Prozessors auf langsame externe Speicher zu reduzieren. Der Cache-Speicher überdeckt dabei ausgewählte Adressbereiche des externen Speichers und enthält die temporär modifizierten Daten sowie damit verbundene Informationen, wie z. B. Informationen zur Lokalisierung der Daten. Eine Übersicht über Cache-Speicher gibt der Artikel 15 von Alan Jay Smith "Cache Memories" in Computing Surveys, Vol. 14, No. 3, September 1982, Seite 473 - 530. Die in Hardware realisierten Cache-Speicher können allgemein als ein Nway-set-assoziatives Speicherfeld charakterisiert werden. Da-20 bei bedeuten die Grenzfälle N = 1 einen Speicher mit Direct Mapping und N = M einen voll-assoziativen Cache-Speicher, wobei M die Gesamtzahl der Einträge im Speicher bedeutet.

Im Allgemeinen werden die Daten in Blöcken von 2^b Bytes pro

Speichereintrag gespeichert. Im allgemeinen Fall eines teilassoziativen Cache-Speichers mit N = 2ⁿ Wegen wird üblicherweise die p Bit breite Adresse des Datums so aufgeteilt, dass
n Bit den Index, b Bit den Offset und die übrigen p - n - b
Bit das Tag bilden. Das ist in der beigefügten Figur veranschaulicht.

Beim Zugriff auf ein Datum im Cache-Speicher, z. B. bei einem Lese- oder Schreibvorgang, wird das Index-Feld verwendet, um ein Set direkt zu adressieren. Das Tag-Feld wird zusammen mit dem jeweiligen Block abgespeichert, um ihn eindeutig innerhalb eines Sets zu identifizieren. Bei einer assoziativen Suche nach dem Block wird das Tag-Feld der Adresse mit den Tag-

Feldern in dem selektierten ner offeet-Rinkran wird henvirat in fenden Rinck aufaufinden reldern in dem selektierten get verglichen, um so den berutzt, um

fenden Block aufzufinden.

fenden Block aufzufinden.

fenden betret
nach aufzufinden. P2001,0019 DE Derartige Cache-Speicher Stellen auf Security-Controllern namit Derartige cache-speicher stellen auf gtrükturen dar.

Derartige cache-speicher ahneenhen von pueleitungen in hilden diese garbe-speicher ahneenhen von pueleitungen v Leicht zu identifizierende regulare strukturen dar. Damit regulare strukturen dar. Damit regulare von Busieitungen in für abgesehen von Busieitunkre für abgesehen von Andriffaninkre für bilden diese hevorzunte nhvaikaliache Andriffaninkre bilden hevorzunte nhvaikaliache pediatereätzen hevorzunte nhvaikaliache pediatereätzen das Datum im Block zu adressieren. Dilden diese Cache-Speicher abgesehen von Busleitungen und

Dilden diese Cache-Speicher physikalische Angriffspunkte für

Registersätzen bevorzugte physikalische Angrifieren von eicherheiter

Registersätzen Angenähen oder Maninulieren von eicherheiter

ein unhefunten Angenähen Registersätzen bevorzugte physikalische Angriffspunkte für nahran oder Manipulieren von ähnliches in Ausspähen oder Manipulieren oder ähnliches ein unbefügtes Ausspähen aurch Madelandriffe oder andriffe oder andr levanten Daten: Z. B. durch Nadelangritte oder Ahnliches. In dernationes achwer and den externen speichern achwer and den externen achwer ac den externen spelchern werden unlicherweise sicherheitskritische Daten die 7 genwer zu decodierende verschlüßselung
sche Daten die 7 genwer zu decodierende verschlüßselung
sche Daten die 7 genwer zu decodierende verschlüßselung
sche Daten die 7 genwer zu decodierende verschlüßselung sche Daten die z. B. in Hardware implementiert entennen A. geschützt. Geschützt. geschutzt, die z. B. in Hardware implementiert sein kann.

Jiese harte Ver- und Entschlüsselung mit entsprechenden zu einer Hardware-Implementierung zu einer Hardware zu einer Ha Diese harte Ver und Entschlüsselung mit entsprechenden zu ei
Diese harte Ver und Entschlüsselung mit entsprechenden zu ei
Tithmen führt auch bei einer Retrieh des Gneichers

Tithmen fistenzzeit im Retrieh rithmen führt auch bei einer Hardware-Implementierung zu eirithmen führt auch bei einer Hardware-Implementierung zu eimer hohen Latenzzeit im Betrieb des Speichers, dan üher
ner hohen Latenzzeit aneichere aniher addiert und dahei den üher
Tatenzzeit des aneichere aniher ner hohen Latenzzeit im Betrieb des Spelchers und dabei veranhlies.

Latenzzeit anreil des Spelchers selbst addiert und dabei veranhlies.

Latenzzeit anreil des Spelchers selbst anreilen kann Latenzzeit des speichers selbst addiert und dabei den übernatenzzeit des speichers selbst addiert und dabei den übernatenzzeit des speichers selbst addiert und dabei der verschlüssenatenzzeit des speichers kann.
Eine derartige
neher rymianherweise in
nateil darstellen kann.
wiegenden under anet. da auf cache-sneicher rymianherweise in
und jet under anet. Wiegenden Anteil darstellen kann. Eine derartige Verschlüsse in warden da auf Cache-Speicher typischerweise in warden da auf Takrauklan augeariffen warden lung ist ungeeignet, wanidan Takrauklan augeariffen augearinden aug Lung 1st ungeelgnet, da aur Cache-Spelcher typlscherwelse in market wenigen Taktzyklen zugegriffen werden, typlscherwelse in and anninkt wenigen Taktzyklen zugegriffen werden, typlscherwelse in anninkt wenigen Taktzyklen zugegriffen werden, typlscherwelse in typlscherwelse in the cache-and characteristics and characteristics and cache-and characteristics and characteristics and cache-and characteristics and characteristics and c 10 einem oder zumindest wenigen gaktzyklen zugegritten werden gchwachpunkt
einem oder zumindest wenigen stellen also einen gemirity-nontrollers
können soll. Cache-Speicher eines derartigen gemurity-nontrollers konnen soll. Cache-speicher stellen also einen schwachpunkt
einen seurity-controllers
derartigen security-controllers
derartigen security-controllers
im sicherheitskonzept eines derartigen neechürzt werden
im sicherheitskonzept anderweitin neechürzt werden anderweitig geschützt werden.

Im Sicnerneitskonzept anderweitig geschützt werden.

dar: Aufgabe der vorliegenden Erfindung ist es eine Möglichkeit nacherung eines cache Aurgabe der vorllegenden erritv-controller angunahen

für eine wirkungsvolle und praktikable sicherungen eines Cache-15 Lur eine Wirkungsvolle und praktikable sicherung einem Security-Controller anzugeben.

Speichers auf einem Security-Controller anzugeben. Diese Aufgabe wird mit dem Verfahren zur Anressierung eine dem Verfahren zur Anressierung eine dem Verfahren zur Anressierung eine Diese Aufgabe wird mit dem Verfahren zur Anressierung eine dem Verfahren zur An Diese Autgabe Wird mit dem Verfahren zur Adressierung eimit dem Verfahren zur Adressierung a. den
mit dem Verfahren des Anspruches ichere mit den Merkmalen des Anspruches des Anspruches des Cache-sneichere mit den Merkmalen des Cache-sneichere mit den Merkmalen des Anspruches des Cache-sneichere mit den Merkmalen den Mer 20 des Anspruches 1 bzw. mit dem Werkmalen des Anspruches anhä

des Cache-Speichers mit den merchen eich aus den jeweiligen
nes Anspruches Anspruchers mit den Merkmalen den jeweiligen anhä nes cache-bperchers mit den werkmalen des Anspruches abhän-löst. Ausgestaltungen ergeben sich aus den jeweiligen abhän-Bei dem erfindungsgemäßen cache-speicher mraneformation zwienhan den die eine umkenrbar eindeutige Transformation zwischen der Adresse und einer verschlüßselten der Adresse und einer verschlüßselten den jeweiligen Tag-Teil der Adresse und einer verschlüßselten gigen Ansprüchen. 30 35

1

5

Tag-Adresse vornehmen. Diese Mittel sind vorzugsweise als Hardware vorhanden. Das erfindungsgemäße Verfahren zur Adressierung wendet eine umkehrbar eindeutige Transformation zwischen einem Tag-Teil einer Cache-Adresse und einer verschlüsselten Tag-Adresse an, was vorzugsweise unter Einsatz von dafür vorgesehenen Mitteln geschieht, die als Hardware vorhanden sind.

Die erfindungsgemäße Lösung gibt durch Mittel und Verfahren eine Methode an, mit der das Sicherheitsniveau von Daten bzw. 10 deren Adressen in Cache-Speichern erhöht werden kann, wobei die Zugriffszeit nicht oder allenfalls unwesentlich erhöht wird. Wie eingangs beschrieben wurde, werden in set-assoziativen Cache-Speichern Daten mittels eines Index-Feldes und eines Tag-Feldes abgelegt und abgerufen. Erfindungsgemäß wird 15 eine umkehrbar eindeutige (ein-eindeutige) Abbildung benutzt, mit der das Tag-Feld der Adresse auf ein verschlüsseltes Tag-Feld abgebildet wird und umgekehrt. Blöcke werden dann im Cache-Speicher zusammen mit dem verschlüsselten Tag-Feld abgelegt. Auf diese Weise ist die Adressinformation für die Da-20 tenblöcke effizient geschützt. Die umkehrbar eindeutige Abbildung wird dabei durch eine dafür vorgesehene Hardware-Einheit durchgeführt. Diese wird bei bevorzugten Ausgestaltungen so ausgelegt, dass die Transformation innerhalb eines Taktzyklusses, d. h. on-the-fly, durchgeführt werden kann. Damit wird die Zugriffszeit auf den Cache-Speicher nicht erhöht.

Als weitere Ausgestaltung der Erfindung kann zusätzlich das

Index-Feld der Adressen des Cache-Speichers durch eine weitere umkehrbar eindeutige Abbildung, die das Index-Feld auf ein
verschlüsseltes Index-Feld abbildet, verschlüsselt werden.
Auch dazu wird eine entsprechend vorzusehende HardwareEinheit verwendet. Damit wird ein sogenanntes Set-Scrambling
erreicht, bei dem der im Cache-Speicher zu verwaltende Block
in einem nicht auf triviale Weise aufzufindenden Set abgelegt
wird. Eine derartige Verschlüsselung wird vorzugsweise dann

zusätzlich durchgeführt, wenn die Architektur des Prozessors nicht vorsieht, dass auf Daten "unaligned" zugegriffen werden kann, so dass die Daten über die Blockgrenzen hinausragen.

Eine erfindungsgemäße Ausgestaltung eines Cache-Speichers ist insbesondere bei Cache-Speichern auf Sicherheitscontrollern (security-controller) bevorzugt.

Patentansprüche

1. Cache-Speicher,

dessen Adressen eine Aufteilung in Tag, Index und Offset auf-5 weisen,

dadurch gekennzeichnet, dass Mittel vorhanden sind, die eine umkehrbar eindeutige Transformation zwischen dem jeweiligen Tag-Teil der Adresse und einer verschlüsselten Tag-Adresse vornehmen.

10

2. Cache-Speicher nach Anspruch 1, bei dem die Mittel zusätzlich eine umkehrbar eindeutige Transformation zwischen dem jeweiligen Index-Teil der Adresse und einer verschlüsselten Index-Adresse vornehmen.

15

3. Verfahren zur Adressierung eines Cache-Speichers, bei dem eine umkehrbar eindeutige Transformation zwischen einem Tag-Teil einer Cache-Adresse und einer verschlüsselten Tag-Adresse vorgenommen wird.

20

4. Verfahren nach Anspruch 3, bei dem zusätzlich eine umkehrbar eindeutige Transformation zwischen einem Index-Teil einer Cache-Adresse und einer verschlüsselten Index-Adresse vorgenommen wird.

Zusammenfassung

Cache-Speicher und Verfahren zur Adressierung

Bei dem Cache-Speicher, dessen Adressen in Tag, Index und Offset aufgeteilt sind, sind als Hardware Mittel vorhanden, die eine umkehrbar eindeutige Transformation zwischen dem jeweiligen Tag-Teil der Adresse und einer verschlüsselten Tag-Adresse vornehmen. Es kann zusätzlich das Index-Feld der Adressen des Cache-Speichers durch eine weitere umkehrbar eindeutige Abbildung, die das Index-Feld auf ein verschlüsseltes Index-Feld abbildet, verschlüsselt werden. Auch dazu wird eine entsprechend vorzusehende Hardware-Einheit verwendet.

	b bit	offset	
,	n bit	index	
	p-n-b bit	tag	

.

}